ISSN (ONLINE) : 2045-8711
ISSN (PRINT) : 2045-869X

# INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY & CREATIVE ENGINEERING

September 2022
Vol - 12 No - 9
@IJITCE Publication

Design by Hemharsith

**UK: Managing Editor**
International Journal of Innovative Technology and Creative Engineering
1a park lane,
Cranford
London
TW59WA
UK

**USA: Editor**
International Journal of Innovative Technology and Creative Engineering
Dr. Arumugam
Department of Chemistry
University of Georgia
GA-30602, USA.

**India: Editor**
International Journal of Innovative Technology & Creative Engineering
36/4 12th Avenue,
1st cross St,
Vaigai Colony
Ashok Nagar
Chennai, India 600083

Email: editor@ijitce.co.uk

**www.ijitce.co.uk**

IJITCE PUBLICATION

# International Journal of Innovative Technology & Creative Engineering

Vol.12 No.09

September 2022

IJITCE
INNOVATE TO CREATE

www.ijitce.co.uk

Dear Researcher,

Greetings!

Articles in this issue discusses about Safety Measures in MANET Using Combined Ids with Data Fusion and Biometrics

We look forward many more new technologies in the next month.

Thanks,
Editorial Team
IJITCE

# Editorial Members

# Contents

# SAFETY MEASURES IN MANET USING COMBINED IDS WITH DATA FUSION AND BIOMETRICS

**Dr. V. K. Narendira Kumar**
*Assistant Professor of Computer Science, PG & Research Department of Computer Science,*
*Gobi Arts & Science College (Autonomous), Gobichettipalayam,*
*Erode District, Tamil Nadu, India.*
*{kumarmcagobi@yahoo.com}*
**Dr. S . Karthigai**
*Assistant Professor and Head in Computer Science,*
*Dr.R.A.N.M. Arts and Science College, Erode, Tamil Nadu, India.*
*{skarthigai@yahoo.com}*

***Abstract - MANETs at the bottom of security-sensitive relevance in aggressive surroundings supplies to be continuously keep an eye on proposed for illegal use. In this paper we study and in attendance the assumption, architecture, implementation and performance of a multimodal combined IDS and Finger print authentication with data fusion providing authentication in a distributed manner. Biometric knowledge provides potential solutions for continuous user-to-device confirmation in high safety mobile ad hoc networks. This paper presents three authentication methods to choose the optimal scheme of combining authentication and intrusion detection. Maintenance and verification of biometric features is the complex task for the personal identification applications. The palm print registration, feature extraction, palmprint verification and palmprint recognition modules are designed to manage the palmprints and the palmprint database module is designed to store their palmprints and the person details in the database. This paper critically reviews and investigates the present biometric based security models works for MANETs, and along with security challenges and direction of further research are proposed.***

*Keyword: - Biometrics, Intrusion Detection, Mobile Ad Hoc Networks (MANETs).*

## 1. INTRODUCTION

Continuous user authentication is an important prevention-based approach to protect high security mobile ad hoc networks (MANETs). Intrusion detection systems (IDSs) are also important in MANETs to effectively identify malicious activities. This paper presents a framework of combining authentication and intrusion detection in MANET. Mobile ad hoc network (MANETs) becomes a popular research subject due to their self-configuration and self-maintenance capabilities. Wireless nodes can establish a dynamic network without the need of a fixed infrastructure. This type of network is very useful in tactical operations where there is no communication infrastructure. However, security is a major concern for providing trusted communications in a potentially hostile environment. This concern is mainly due to the peer-to-peer architecture in MANETs, system resource constraints, shared wireless medium, and highly dynamic network topology [1]. Two complementary classes of approaches exist to protect high security MANETs, prevention-based approaches, such as authentication, and detection-based approaches, such as intrusion detection [2].

The rapid growth in the use of Internet applications and the great concern of security require reliable and automatic personal identification. Several identification and verification schemes that exist today but the most accurate identification is in the area of biometrics. Some examples of identifying biometric characteristics are fingerprints, hand geometry, retina and iris patterns, facial geometry, and signature and voice recognition. The authors in [9] proposed a useful

framework to combine user authentication and intrusion detection. This paper studies three techniques for combining authentication and intrusion detection in MANETs. Dynamic programming based hidden markov model algorithm used to derive the optimal scheme [9]. The partially observable Markov decision process (POMDP) [10] and relevant algorithms can be used solve the combined intrusion detection and continuous authentication problem. Optimal scheme is chosen based on the information state.

**Two interesting properties of biometric identification are:**

1. The person to be identified is required to physically be present at the point of identification.
2. Identification is based on the biometric technique that does not depend on the user to remember a password or to carry a token.

**There are two distinct functions for biometric devices:**

1. To prove you are who say you are
2. To prove you are not who you say you are not.

The purpose of the first function is to prevent the use of a single identify by multiple people (e.g. a possible attacker or attackers attempting to take over the plane cannot pass themselves off as a registered pilot). In this case it is important that the biometric device be able to differentiate between a live biometric presented to the scanner (i.e. a real finger or a spoofed biometric trying to fool the scanner). The second function is used to prevent the use of multiple identities by a single person. It would have to be ensured that the biometric system either automatically cross checks the enrolled characteristics for duplicates, or otherwise does not allow a person to register their biometric under two different names.

The personal identification system using palmprints is designed to carry out the palmprint recognition and verification operations. The system uses the ordinal measurement for the recognition and verification tasks. The color intensity and brightness values are used in the system. The region based ordinal measurement estimation is used in this system [1]. The system does not consider the orientation factors for the palmprint comparison. Palm print recognition and verification schemes are used for the personal identification process. The proposed system is designed to perform the personal identification process using palm prints. Security is primary concern in MANETs and in order to achieve high security (confidentiality, integrity, authentication, availability and non repudiation), several techniques have been explored in which bio metrics with cryptography or intrusion detection has gained a momentum in recent years.

## 2. OBJECTIVES OF THE SYSTEM

In MANETs, a malicious node can launch deny of service (DOS) or disrupt the routing mechanism by generating error routing messages. For these types of attacks, intrusion detection can serve as a second wall of defense and is of paramount importance in high security networks. An IDS continuously or periodically monitors the current subject activities, compares them with stored normal profiles and/or attack signatures, and initiates proper responses [9]. Two main technologies of identifying intrusion detection in IDSs are given as follows: misuse detection and anomaly detection. Misuse detection is the most common signature-based technique, where incoming outgoing traffic is compared against the possible attack signatures/ patterns stored in a database. If the system matches the data with an attack pattern, the IDS regards it as an attack and then raises an alarm. The main drawback of misuse detection is that it cannot detect new forms of attacks. Anomaly detection is a behavior-based method, which uses statistical analysis to find changes from baseline behavior. This technology is weaker than misuse detection but has the benefit of catching the attacks without signature existence. Person identification system is designed to perform the person identification operation using the palmprints. The palmprint recognition and verification are the main objectives of the system. The ordinal measures can be used to rank and order the palmprint images. The system should perform the recognition and verification operation orientation independently. The region based comparison technique can be applied for the system. The ordinal feature and edge feature are the main features for the palmprint recognition process. The orientation independent personal identification process is the main motive for the system. The person identification with palmprint recognition and verification is the design goal of the system.

## 3. MANET APPROACH

MANET has a continuous authentication system, which is equipped with multiple biosensors and has the ability to collect multiple biometrics, and IDS, which has the ability to detect

intrusions. The time axis is divided into slots of equal duration that corresponds to the time interval between two operations. The length of time slot depends on the security requirements and the system environment. IDS is continuously monitoring the system, the IDS is operated at all time instants. An authentication may be initiated at every time instant as well. The IDS and authentication may consume extensive system resources, such as battery power, which is an important issue in MANETs. Therefore, it is desirable to optimally schedule intrusion detection and authentication at each time instant taking into account system security requirements and resource constraints. Markov model is a very popular approach [10], used in solving security problems. There are several biosensors used for continuous authentication and several sensors used for intrusion detection. In this case, both an IDS and an authentication can be run simultaneously. Let uk ∈ {1, . . ., L} denote the sensor selected at time k, and yk(uk) denote the observation of this sensor. The observations of the lth sensor belong to a finite set of symbols {O1(l),O2(l), . . . , OMl (l)} and |Ml| denotes the number of possible observations of the lth sensor. When the system state is ei, the lth sensor is picked at time k, the probability of observation m will be obtained from the lth sensor is denoted as: bi(uk = l, yk = Om(l)).

The partially observable Markov decision process (POMDP) [10] and relevant algorithms can be used solve the combined intrusion detection and continuous authentication problem.

An information state is a sufficient statistic for the history, which means that the optimal sensor (i.e., the optimal operation, intrusion detection or authentication) can be chosen based on the information state, denoted by πk, where k is the time. System procedure can be briefly summarized as three steps,

a. Scheduling: Based on the information state πk, find the optimal sensor uk+1 that will be used at the next horizon.

b. Observation: Observe the output of the optimal sensor yk+1(uk+1) at next horizon.

c. Update: Update the information state πk+1 using the latest observation yk+1.

Palm identification, just like fingerprint identification, is based on the aggregate of information presented in a friction ridge impression. This information includes the flow of the friction ridges the presence or absence of features along the individual friction ridge paths and their sequences and the intricate detail of a single ridge. To understand this recognition concept, one must first understand the physiology of the ridges and valleys of a fingerprint or palm. When recorded, a fingerprint or palmprint appears as a series of dark lines and represents the high, peaking portion of the friction ridged skin while the valley between these ridges appears as a white space and is low, shallow portion of the friction ridged skin.

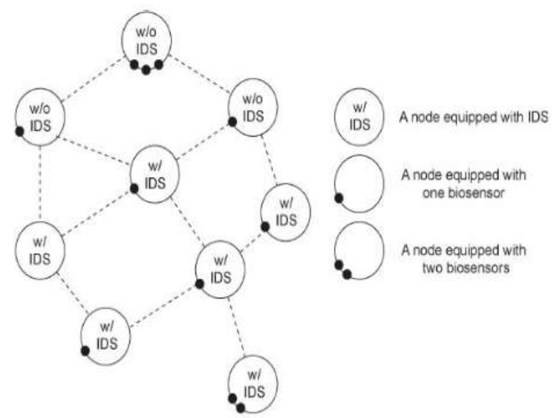


**Fig.1 MANET having Nodes Equipped with IDS and Biosensors**

A host based IDS rely on system audit data to monitor and analyze the events generated by programs or users on the host. In the system aspect, individual IDS are p laced on each and every node. Each IDS node runs independently and monitors local activities. If anomaly is detected in local data or data is inconclusive and border search is warranted, neighboring IDS will corporately participate in global intrusion detection actions. These individual IDS agents collectively form the IDS system to defend the wireless ad hoc network. Palm recognition technology exploits some of these palm features. Friction ridges do not always flow continuously throughout a pattern and often result in specific characteristics such as ending ridges or dividing ridges and dots. A palm recognition system is designed to interpret the flow of the overall ridges to assign a classification and then extract the minutiae detail a subset of the total amount of information available, yet enough information to effectively search a large repository of palmprints. Minutiae are limited to the location, direction and orientation of the ridge endings and bifurcations' (splits) along a ridge path. A pictorial representation of the regions of the palm, two types of minutiae, and examples of other detailed

characteristics used during the automatic classification and minutiae extraction processes.

## 4. DATA FUSION OF BIOMETRIC SENSORS AND IDS

In the proposed scheme, L sensors are chosen for authentication and intrusion detection at each time slot to observe the security state of the network. To obtain the security state of the network, these observation values are combined, and a decision about the security state of the network is made. However, since there is some probability that a given sensor might either be in a compromised state or have made an inaccurate assessment, it is possible that this sensor has contributed an unreliable observation. It can be quite difficult to ascertain which observers are compromised. Therefore, choosing an appropriate fusion method is critical for the proposed scheme. The decision about which sensors are chosen should not totally depend on the current observation values since the sensors' states are only partially observable. This paper based on the strategy that if the sensors are trustworthy, it always provide accurate observation data. Any chosen node could be untrustworthy due to its current compromised state or inaccurate detection. The chosen node n is trustworthy for an arbitrary observed node a at time slot k + 1 when it is in the secure state and accurately detects. The trustworthy probability tp k+1(n) of node n at time k + 1 is equal to P(sk+1n= secure) × P(yk+1(n) = s k+1α), where y(n) k+1 is the observation of a's security state obtained from node n. In our scheme, P(y(n) k+1 = secure|sα k+1 = secure) and P(yn k+1 = compromised|sa k+1 = compromised). Biometrics makes use of the physiological or behavioral characteristics of people such as fingerprint, iris, face, palmprint, gait, and voice, for personal identification, which provides advantages over non-biometric methods such as password, Personal Identification Number, and ID cards [3].

Palmprint is the unique inner surface pattern of human hand, including a number of discriminating features, such as principal lines, wrinkles, ridges, minutiae points, singular points, texture etc. Compared with other biometric traits, the advantages of palmprint are the availability of large palm area for feature extraction, the simplicity of data collection and high user acceptability.

Various palmprint representations have been proposed for recognition such as Line features, Feature points, Fourier spectrum, Eigen palms features, Sobel's and morphological features, Texture energy, Wavelet signatures, Gabor phase, Fusion code, Competitive code, etc.

The system is attempt to explore a convincing solution, that of using ordinal measures, as an answer to the representation problem. The representation of ordinal measures unifies several state-of-the-art palmprint recognition algorithms of David Zhang. The internal representations of those algorithms can be seen as special cases of ordinal measures. This form a framework, which may help to understand the discriminate power of palmprint pattern, guide further research and enlighten new ideas.

## 5. UNIFIED FRAMEWORK FOR PALMPRINT RECOGNITION

A general framework of palmprint recognition is based on the ordinal representation is proposed. To input a palmprint image, the central sub image in the aligned coordinate system is cropped from it for feature extraction. To obtain the special measurements for ordinal comparison, the normalized palm image is transformed to feature image. Then the ordinal measures are obtained by qualitatively comparing several quantities in feature image. In practice, the transformation and ordinal comparison can be combined into one step via differential filtering. The result of ordinal comparison may be the sign of an inequality, the rank order of all measurements involved in comparison, maximum or minimum value associated index and so on. After ordinal comparison, all results are coarsely quantized into binary bits so as to strengthen the robustness of palm feature and facilitate matching step. All binary codes are concatenated to generate a palmprint feature, which is the input of matching engine. Finally, the dissimilarity between the input palm print's ordinal feature and the template stored in database is measured by their Hamming distance.

**The framework has some desirable properties for palmprint recognition:**

- The ordinal measure renders the palmprint representation robust against various intra-class variations such as illumination settings, dirties or sweats on palm, signal noises, pose change, misalignment and nonlinear deformations [4].
- The palm print template is compact. Thousands of ordinal comparison results

needs memory less than 1K bytes, which provides the possibility to store the palmprint template in IC card, mobile phone or PDA.

- The dissimilarity between two palm prints can be measured by bitwise XOR operator, which could be computed on-the-fly [8].

## 6. SYSTEM DEVELOPMENT

The proposed systems are necessarily the best solution taking into account different applications. Every organization should choose the appropriate IDS for its network. Moreover, it can change the IDS according to its own requirements and characteristics. For example, it can change architecture of chosen IDS or put different intrusion detection techniques together. Therefore, defining requirements and determining characteristics of the network are very important factors in determining the most appropriate IDS solution. The personal identification using palmprint system is developed as a graphical user interface based tool. The system is developed using the J2EE language and the Oracle relational database. Palmprint features and person details are maintained in the database. The palmprint images are maintained with their id. A separate folder is allocated to maintain the palmprint images.

The palmprint images are captured in two ways. They are image scanners and thermal scanners. The thermal scanners are used to capture the palmprint images directly from the hand. The image scanners are used capture the palmprint images from pictures. The images are maintained in two formats. They are Joint Photographical Expert Group (JPEG) and Graphical Interchange Format (GIF). The palmprint images are divided into 4 x 4 regions. The 16 regions are used for the feature extraction process. The color brightness and intensity values are used for the feature extraction process. The feature values are maintained for each image under the database. The verification process is done with the person id and the palmprint image. The recognition process is carried out with the palmprint image only. The verification and recognition operations are conducted with a threshold value for the similarity rate estimation process.

## 7. SYSTEM IMPLEMENTATION

The palmprint verification and recognition system is implemented to perform the person identification operations. The palmprints are one of the important biometric features that are used to identify a person with unique properties. The palmprint and relevant person details are maintained in the database. Palmprint features such as line, edge, ridge and orientation features are maintained in the database. This system uses a new feature named as dominal features. The dominal features are extracted with reference to the color and texture properties.

The person identification task is divided into two types. They are biometric verification and recognition operations. The palmprint is used as the biometric features for the person. The verification process performs the similarity checking for the given person id and the palmprint image. The palmprint database image for the specified person is compared with the input image. The verification process requires only one comparison process. The recognition is the process of identifying an unknown person with reference to the biometric features. In this mechanism the palmprint database images are compared with the given input image. Most relevant image is referred as similar palmprint for the person.

The person identification using palmprints is developed as a graphical user interface based application. The Java language is used as the front end and the Oracle relational database is used as the back end for the system. The system is divided into four major modules. They are palmprint database, feature extraction, verification and recognition. The palmprint database module is designed to manage the palmprint and person details under the database. The feature extraction module is designed to fetch the ordinal and line features for the palmprints. The palmprint verification for the given person is performed in the verification module.

### A. PALMPRINT DATABASE

The palmprint database module is the initial module in this application. The personal detail and palmprint data are maintained in the database. Palmprints are maintained as image files. The palmprint database updates the palmprint image name under the database. The palmprint database also maintains the color and ordinal features in the database. The ordinal values for 16 regions are maintained in the

database. The system also maintains the rank or order for the palmprints with reference to its ordinal values. The ranking values are used in the recognition process. The person details and ordinal features are maintained in two different tables [5].

The palmprint database module is divided into three sub modules. They are palmprint registration, palmprint list and palmprint view. The palmprint registration sub module is designed to register a person details with the palmprint information. The person name, address, city, state, country and e-mail details collected and updated into the database. The system assigns a unique person identification number for the registered persons. The palmprint image path is also registered into the palmprint registration process [9]. The palmprint is copied into the images folder maintained in the application path. The palmprint image is renamed with reference to the person identification number assigned by the system.

The file open dialog window option supports the palmprint path selection process. The user can easily select the path for the palmprint image. The palmprint list sub module shows the list of registered person details with the palmprint details. The palmprint list is prepared by using the palmprint database. The palmprint image view sub module is designed to print the palmprint for the selected person from the palmprint list.

## B. FEATURE EXTRACTION

The feature extraction module is designed to extract and update the palmprint image features. The recently updated palmprint image features are extracted and updated under the database. The color and texture feature are the main feature that considered in this system. The color and texture feature is referred as ordinal features. The line features are used for the comparison process. The palmprint image pixel values are used for the feature extraction process. The color brightness and intensity values are used for the feature extraction process.

The feature extraction module is divided into two sub modules, feature identification and ordinal measurement. The feature identification process is carried out over the regions on the palmprint images. The palmprint image is divided into 4 x 4 regions. All the 16 image regions are passed into the feature extraction process. The color intensity and brightness for each block is compared with another palmprint image. The ordinal values are estimated with reference to the color brightness and intensity values. The ordinal values are represented as 0's and 1's. The block ordinal value is summed and they are compared with the similar block in the other palmprint image. The comparison results are also maintained as 0's and 1's. The total ordinal measure for the image is calculated and assigned for the image. The ordinal measurement sub module displays all the ordinal measurements and ratio level for each image.

## C. PALMPRINT VERIFICATION

The palmprint verification module is designed to carry out the person's identification tasks. The verification process performs the palmprint comparison process only one iteration [10]. The person id and input palmprint image are collected from the user. The palmprint selection module is designed for the palmprint selection process. The feature for the input palmprint is extracted and compared with the palmprint image features that are maintained for the relevant person under the database. The feature comparison module is designed to carry out the comparison process [6]. The ordinal features and line features are used for the feature comparison process. The false acceptance ratio and false rejection ratio are used for the comparison process. The final result of the verification process is given as the palmprint which is similar to the referred person.

## D. PALMPRINT RECOGNITION

The palmprint recognition module is designed to carry out the person identification process for the unknown person. The palmprint image is the only input data for the recognition process. The person identification details are the expected output value. The input image feature is compared with the database image features. The relevancy is estimated with reference to the threshold value. The most relevant image is selected for the person's identification. If the comparison result does not match with the input image then the recognition process is declared as unknown person.

The recognition module is divided into four sub modules. They are palmprint selection, result details, ordinal list and ordinal measurement. The palmprint image selection sub module is designed to select the palmprint input image. The file open dialog is used to select the input image file. The result details produce the list of relevant palmprint with their similarity ratio details. The ordinal list shows the ordinal feature based comparisons. The

ordinal measurement sub module shows the ordinal values for each region.

## 8. LIVENESS TESTING

Some biometrics can be fooled by presenting an artificial or simulated biometric sample. What is required for protecting against these attacks, is *liveness testing:* an automated test performed to determine if the sample presented to the system comes from a live human being.

**Consider Examples for palmprint:**

A palmprint scanner by Sony FIU-500 is an optical sensor. However, it tests for liveness by measuring the capacitance of the skin. If it is not within norms, the sample is rejected.

A method developed at West Virginia University captures the perspiration pattern using a capacitive palmprint scanner. Live palm sweats, pores fill with moisture, and the capacitance changes. The measurement is done in 5 seconds.

**Other things than capacitance can be measured:**

- **Properties of a living body:**

***Mechanical:*** weight, density, elasticity. ***Electrical:*** resistance, impedance, dielectric constant.
***Visual:*** color, opacity, appearance.

- **Signals generated by a living body:**

Pulse, blood pressure, heat, thermal gradients, electrical signals generated by the heart, etc.

- **Responses to a stimulus:**

***Voluntary:*** Tactile, visual.
**Auditory:** respond to feeling/seeing/hearing something.
***Involuntary:*** Electromyography, pupil dilation, reflexes.

### A. Performance Measures

Performance testing is the process by which software is tested to determine the current system performance. This process aims to gather information about current performance, but places no value judgments on the findings. The proposed tests will measure the following aspects of performance.

- Failure to enroll rate.
- Failure to acquire rate.
- System false match and false non-match rates.
- User throughput.
- Matching algorithm throughput (reported with processing system used).
- Sensitivity of performance to (potentially problematic) changes in environment, population or usage.

## 9. EXPERIMENTAL RESULTS

MANETs are a new type of distributed network whose properties are complex and ill-understood. Intrusion detection on these complex systems is still an immature research area. There are far fewer proposed IDSs for MANETs than for conventional networks. Researchers can focus on either introducing new IDSs to handle MANET specific features or can adapt existing systems. Hybrid approaches may also prove of significant use. Palmprint images from 284 individuals using the palmprint capture device as described in [7] are collected. In this dataset, 186 people are male, and the age distribution of the subjects is: about 89% are younger than 30, about 10% are aged between 30 and 50, and about 1% is older than 50. The palmprint images were collected on two separate occasions, at an interval of around two months. On each occasion, the subject was asked to provide about 10 images each of the left palm and the right palm. Therefore, each person provided around 40 images, resulting in a total number of 11,074 images from 568 different palms in our database. The average time interval between the first and second occasions was 73 days. The maximum and the minimum time intervals were 340 days and 1 day, respectively. The size of all the test images used in the following experiments was 384´284 with a resolution of 75dpi. The database is divided into two datasets, training and testing. Testing set contained 9,599 palmprint images from 488 different palms and training set contained the rest of them.

The training set is used to adjust the parameters of the Gabor filters only. All the experiments were conducted on the testing set. We should emphasize that matching palmprints from the same sessions was not counted in the following experiments. In other words, the palmprints from the first session were only matched with the palmprints from the second session. A matching is counted as a genuine matching if two palmprint images are from the same palm; otherwise it is counted as an imposter matching. Number of genuine and imposter matching are 47,276 and 22,987,462 respectively.

A feature-level coding scheme for palmprint identification is presented. On the top of PalmCode [7], a number of improvements for developing Fusion Code are made. 1) The circular

Gabor filter in PalmCode is replaced by a bank of elliptical Gabor filters. 2) A feature level fusion scheme is proposed to select a filter output for feature coding. 3) The static threshold in PalmCode is replaced by the dynamic threshold. A series of experiments has been conducted to verify the usefulness of each improvement.

## 10. CONCLUSION

Continuous authentication and intrusion detection jointly improve the security performance of the MANET. This paper, presented a distributed scheme combining authentication and intrusion detection. Dempster–Shafer theory has been used for IDS and sensor fusion since more than one device is used at each time slot. The distributed multimodal biometrics and IDS scheduling process can be divided into offline and online parts. In the structural result method, the optimal policy can be chosen based on the getting index. Structural results method used for calculating the Getting indices of the sensors in a large network with a variety of distributed nodes. Intrusion detection is modeled as noisy sensors that can detect the system security state (safe or compromised). Continuous authentication is performed with multimodal biometrics. This paper presents the comparative study of different techniques which is used to combine authentication and intrusion detection. The person identification system uses the palmprint biometric feature to identify a person uniquely. The palmprint images applied into the transformation and ordinal measurement evaluation process. The ordinal measures are used to rank and order the palmprint images. The system performs the region based comparison mechanism to carry out the recognition and verification operations. The palmprint database is updated with a set of personal details and palmprint image collection. The feature extraction process is verified and the ranking process is also validated. The palmprint recognition and verification operations are tested with a set of sample image collections. The ordinal measures and similarity ratio are estimated and verified for each analysis process. The similar palmprints are identified with high similarity ratio and irrelevant palmprint images are not recognized by the system. The system provides the palmprint recognition mechanism without the orientation related factors. The ordinal measurement based upon the person's identification mechanism is a feasible solution for the personal identification requirements. In order to implement this personal identification system using palmprint efficiently, J2EE language and the Oracle relational database is used. This program could speed up the development of this system. Future work is to consider more nodes' states in making the scheduling decisions in MANETs and also to increase the network life time.

## References


[1] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Securing mobile ad hoc networks with certificateless public keys," IEEE Trans. Depend. Secure Comput, vol. 3, no. 4, pp. 386-399, Oct./Dec. 2006

[2] H. Yang, H. Luo, F. Ye, et al., "Security in mobile ad hoc networks: challenges and solutions," IEEE Wireless Commun., vol. 11, no. 1, pp. 38-47, Feb. 2004.

[3] A. Weimerskirch and G. Thonet, "A distributed light-weight authentication model for ad-hoc networks," Lecture Notes in Computer Science, vol. 2288, pp. 341-354, ISBN: 3-540-43319-8, 2001.

[4] Q. Xiao, "A biometric authentication approach for high security ad-hoc networks," in Proc. IEEE Info. Assurance Workshop, West Point, NY, June 2004.

[5] Anil K. Jain, Patrick Flynn and Arun A. Ross "Handbook of Biometrics" Springer; 1 edition 2007

[6] D.D. Zhang "Palmprint Authentication" Publisher: Springer; 1 edition 2004

[7] S.Bu. F. Yu, P. Liu,"Structural Results for Combined Continuous UserAuthentication and IntrusionDetection in High Security Mobile Ad-Hoc Networks,"IEEE Wireless Commun, vol. 10, no. 9, Sep 2011.

[8] John D. Woodward Jr. and Nicholas M. Orlans "Biometrics" McGraw-Hill Osborne Media; 1 edition 2002

[9] John R. Vacca "Biometric Technologies and Verification Systems" Butterworth-Heinemann; 1 edition 2007

[10] K.S. Thyagarajan "Digital Image Processing with Applications", Focal Press, 2005.

[11] Kenneth R. Castleman "Digital Image Processing" IPrentice Hall 1995.

[12] Patricia Anne Kolb "H.I.T: A manual for the classification, filing, and retrieval of palmprints" Publisher: Thomas 1979

*[13]* Samir Nanavati, Michael Thieme and Raj Nanavati "Biometrics: Identity Verification in a Networked World" Publisher: Wiley; 1st edition 2002.


September 2022
Vol - 12 No - 9
@IJITCE Publication